CHAPTER 3. Requirements

Management Services

Management Services is defined as the ability to manage all hardware and software resources in a heterogeneous, distributed information system. Efficient and effective management of DII is extremely important to the functional user community supporting the defense of the United States. Maintaining operations of a vast and diverse array of information resources interconnected with Local Area Networks (LAN) and Wide Area Networks (WAN) is a major undertaking; however with strict guidelines and robust tools the task will be better handled. The purpose is to ensure that the information systems continue to operate in support of the efforts of the warfighters and supporting organizations during peace-time, crisis and war-time operations. This document addresses and defines the functions and requirements of the Management Services within the DII COE.

Management Services includes the following areas, which are often implemented separately due to the lack of integrated tools:

1. Network Administration: Network Administration is defined as those services that support the configuration of network elements, establishment of network connectivity, and ensuring continuous network operations.
2. System Administration: System Administration is defined as the services that are required to ensure effective and efficient operation of those elements of the information system that are not an integral part of the network and to manage the configuration and operations of workstations, servers, applications and the user environment on a day-to-day basis.
3. Security Administration: Security Administration is defined as the services required to manage, configure, operate and maintain information system security functions and to ensure that the system continues to meet security requirements as defined by the accrediting authority.

This document identifies the functional requirements for management services to support these three areas. Because these areas are interdependent, the requirements are addressed in terms of management services as an integrated set of functions. These functions include the five System Management Functional Areas (SMFAs) defined by the International Organization for Standardization (ISO): configuration management, fault management, performance management, security management, and accounting management. However, since accounting management entails functions necessary for charging fees to users for the use of system resources, and it is not the intention of the government to need those capabilities, accounting management will not be addressed further in this document.

Management Services are provided in accordance with Management Domains as defined by the ISO. A management domain is a bounded set of information system resources that are under the management and control of a single set of management tools. Three levels of management have been defined for DII: (descriptions of global, campus and site to be added). There is a single manager for the global level, while the campus and local levels will be implemented numerous times depending on Command and site configurations. Each implementation constitutes a management domain.

Communications Services

Communication Services provide for various modes of communication between parts of distributed applications. Communications Services also provide services such as Combat Net Radio and broadcast services and high level communications protocols such as SMTP, FTP and Telnet. Communication Services provide the reliable, transparent, end-to-end data communications.

The boundary that defines Communications Services is the "wire" on one end and a "memory buffer" or consumer (client) on the other. For example, the GCCS must have the ability to send and receive data from external systems. Communications Services serve as the boundary between such systems and are responsible for getting the data "off the wire" for subsequent use by the Message Processing Services. As another example, a COE server needing to establish a connection with a peer server located on another workstation will use Communications Services to exchange data across the network.

The functional capabilities or high level system requirements of Communications subsystem are listed without reference to actual government-off-the-shelf (GOTS) products being developed or in the field today. This keeps this document at a notional level vice being a description of a particular product (or products).

Security Services

The security requirements contained within this document are a reflection of the DOD security policy and operational considerations, and assist systems in accomplishing their mission.

The security services for the DII COE can be broadly categorized into the following six areas:

1. **Accountability.** The property that enables security relevant activities on a system to be traced to individuals who may then be held responsible for their actions (NCSC, 1988).
2. **Access Control.** The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.
3. **Confidentiality.** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
4. **Integrity.** The property that information has not been altered or destroyed in an unauthorized manner.
5. **Non-repudiation.** The proof of delivery or origin of information transactions.
6. **Availability.** The state when data is in the place needed by the user, at the time the user needs them, and in the form needed by the user (NCSC, 1988).

The level of assurance[1] necessary to determine if these services have been implemented correctly is a function of many factors. These factors are specific to the system that is being built with COE components and difficult to pre-determine. However, the sensitivity of the data being processed on the system and the clearance levels of system users are two factors that must always be considered. Over time, selected COE components will be selected that have higher assurance. Assurance requirements are included in section SEC 3.12, SEC 3.15, and SEC 3.16. Section SEC 3.12 includes requirements that are related to the design and specification of security functionality, section SEC 3.15 includes requirements for configuration management, and section SEC 3.16 includes requirements related to security testing of that functionality.

3.1 Required States and Modes

3.1.1 Management Services

The DII operates in the following modes:

- **Operational Mode**. This is the normal mode of operation where the DII is on-line supporting the operational mission.
- **Maintenance Mode**. In this mode, portions of the hardware or software at the DII site will be off-line for maintenance, modification, upgrade, or other related action.

[1] Assurance is a measure of confidence that the security features and architecture of the COE accurately mediate and enforce the security policy (NCSC, 1988).

- **Training Mode**. In this mode, a portion of the DII may be operated with separate databases using simulated inputs in support of training for a portion of the user population. Care must be taken to ensure that exercise data is not mixed with operational data.
- **Exercise Mode**. In this mode, a portion of the DII may be operated with separate databases using simulated inputs in support of an exercise for a portion of the user population.

Care must be taken to ensure that exercise data is not mixed with operational data. Normal day-to-day operations will probably find all four operating modes existing at the same time at different DII sites. The modes will be distinguished by administrative features or architectural boundaries. The Management Services requirements are valid for all required states and modes.

3.1.2 Security Services

The security services requirements are applicable to all operational modes, including, but not limited to training, emergency, backup, wartime, peacetime, idle, ready, and active. The security services software will remain the same during any operational mode.

3.1.3 Communications Services

Communications Software shall operate in more than one state. Each state may have multiple modes of operation. The attributes and characteristics of each state and shall be identified and described in the Software Description Document (SDD). Communications software shall consist at least but not limited to the three states as described below**:**

1. **Startup State**: This state shall commence when Communications Software is initially executed. This state shall consist of a single mode during which power -up test of communications hardware are performed. This state shall terminate when hardware tests are completed.
2. **Initial Download State**: This state shall commence after the Startup State is completed. This state consist of a single mode during which communication software components are being downloaded to Communications devices., Communications Software shall allow the users, application software, or higher layer software to configure and initialize or alter the network configuration parameters prior to the network operation.
3. **Operational state**: This state shall commence after the Initialization State is completed. In this state, Communication Software shall be capable of sending and receiving messages. This state may consist of multiple operational modes such as: Inactive Mode (Fault or Degraded mode), Configuration mode, Standby Mode, Normal Operational Mode, and Training Mode.

3.1.3.1 Network Management Services

The Network Management Functional Area is not a stand-alone subsystem. NM oversees the connectivity between DII users via the SIPRNET and is designed to be transparent to the DII users. The Network Management Functional Area has no operating modes or states of its own.

The DII operates in three modes. The first is On-Line. This is the normal mode of operation where the DII is on-line capable of performing its operational mission. The second is a Maintenance mode. In this mode portions of the hardware or software at a DII site will be off-line. This may be due to a hard equipment failure or for routine maintenance. The third mode of operation is Exercise. In this mode a portion of the DII may be operated with separate data bases using simulated inputs. This could be for war gaming purposes or for testing new functionalities for the DII. It is important to understand these modes of operation are not mutually exclusive. In fact, normal day-to-day operations will probably find all three operating modes existing at the same time on different portions of the DII. The different modes will be distinguished by administrative features or architectural boundaries.

3.1.4 Distrbuted Computing Services

No discussion necessary since the required modes and states are documented for the entire COE.

3.1.5 Data Management (Data Access) Services

The DAS functional area will need to operate in more than one state or mode, each having unique attributes and characteristics. These characteristics are used to define the state or mode of operation, and may be found in Tactical or Strategic military situations.

Different modes of operation include:

- Dynamic or Static
- High Speed or Low Speed
- High Quality or Low Quality.

In the military environment a High Speed mode of operation is typical for the strategic planning and theater-level command and control environment. Its operational mode is based on a fixed computing client-server environment with fixed high-speed reliable communications between clients and servers.

A typical military environment in a Dynamic mode of operation is that of the tactical command and control military environment. It needs to function in a mode of dynamic connectivity based on a client-server environment, consisting of limited communications where the communications media is either wired or wireless. The communications media can be of variable bandwidth, and of variable reliability between nodes, with possible communications dropouts. Special requirements are needed in this operational mode for authentication of communications connections.

In addition there are several states in which the COE DAS functional area will operate in. These states will define the runtime state of the system regardless of the mode or echelon of the system. The states are:

- Training
- Configuration
- Operational
- Stand By
- Fault or Degraded.

In the training state the corresponding operational environment is simulated and a duplicate training environment is created to train the end-users in a system identical to that of the operational environment. The system is set up so that a parameter controlled by an operator at the console enables connectivity to a training database. For example, in a military environment end-users need to be trained in the exact operational system they will use, where the only differences are that the training state requires that the actual data being used, as well as the control messages exchanged, are clearly defined to be training test data and messages.

3.1.6 Presentation Services.

The states and modes in which presentation systems and services operate will be determined by the higher-level application software that uses it, and is therefore transparent to this area. Similarly, the presentation systems and services will be driven by available hardware and communications (e.g., video teleconferencing may not be available on all workstations, low bandwidth users may only have access to text browsers).

3.2 Functional Requirements

The following sections describe the functional requirements for Management Services and System Administration Services; Security Services (including Security Administration Services); Communications Services and Network Services; Distributed Computing Services; Data Management Services; and

Presentation Services (including the Executive Management functional area and the Multimedia functional area).